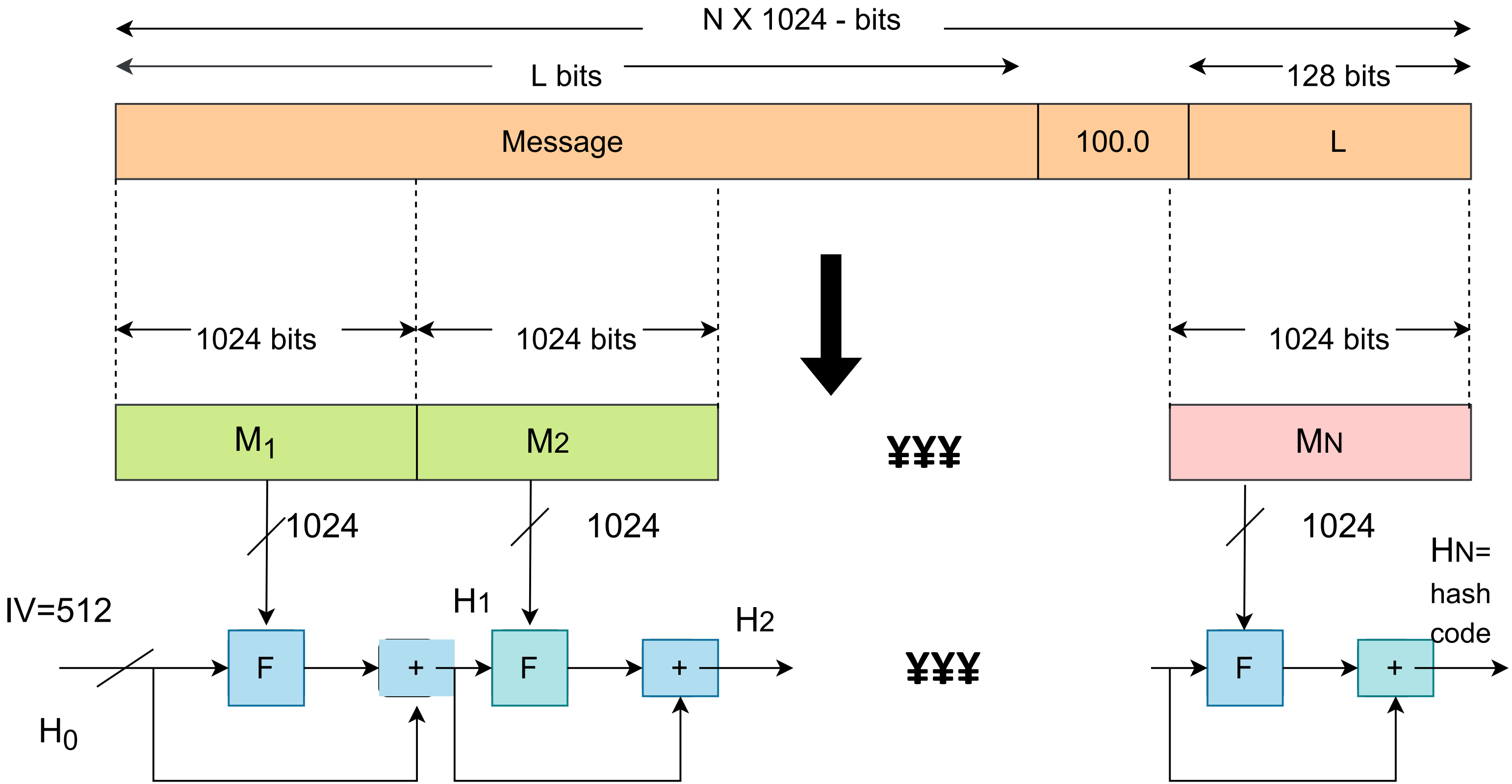
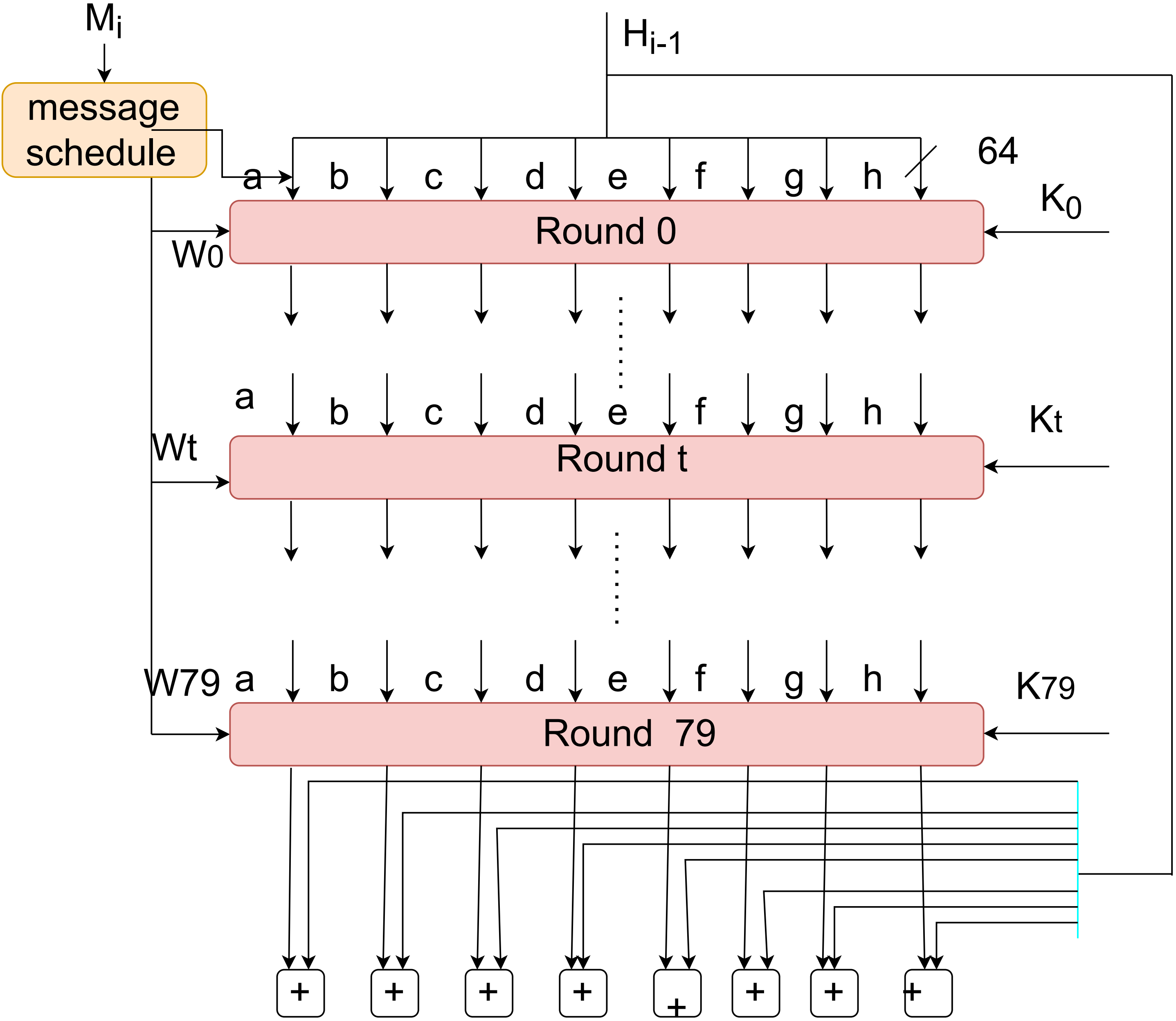
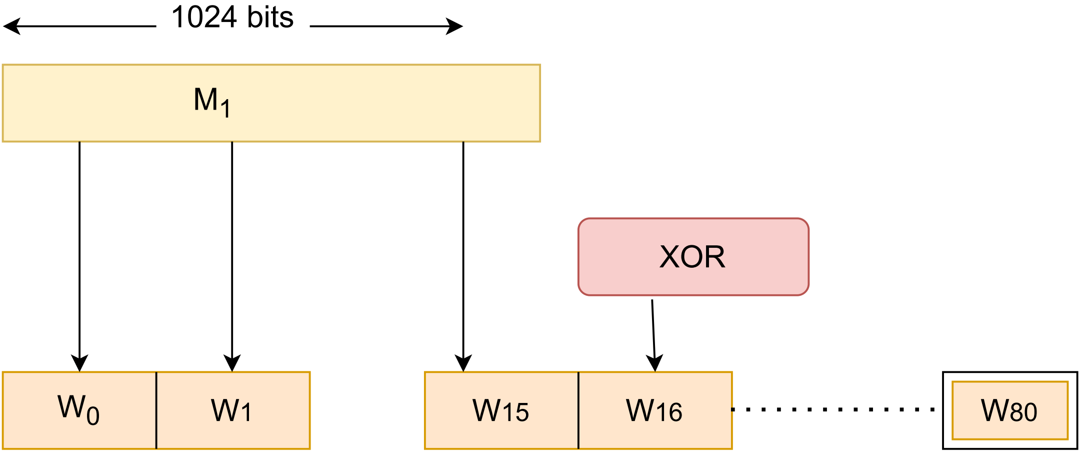
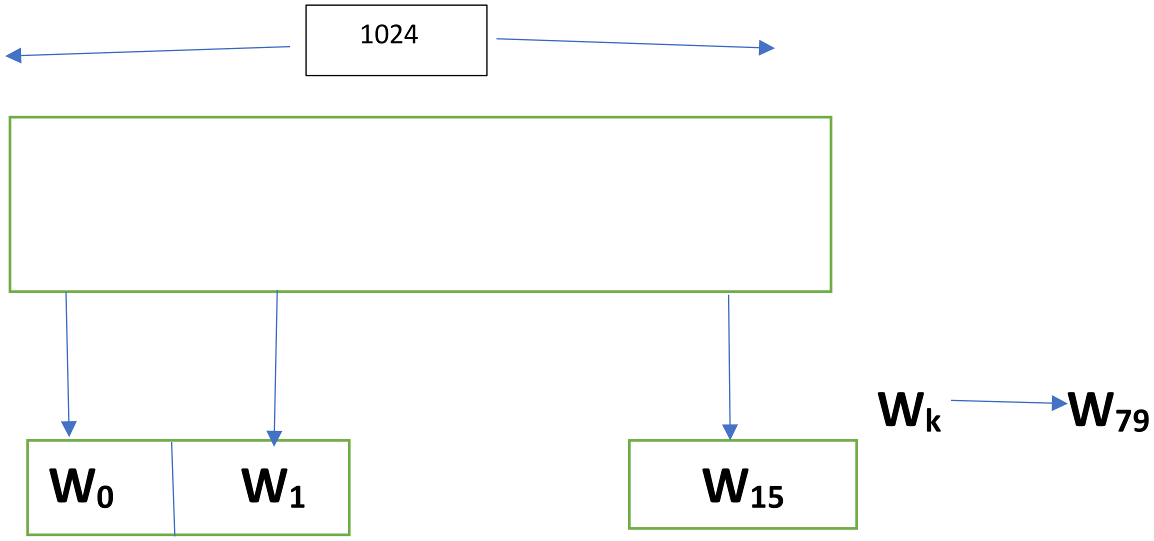

N X 1024 - bits
L bits
128 bits
Message
100.0
L
1024 bits
1024 bits
1024 bits
M1
M2
¥¥¥
MN
1024
1024
1024
HN=
hash
code
IV=512
H1
H2
F
+
F
+
¥¥¥
F
+
H0


M_i
message schedule
H_{i-1}
64
a
b
c
d
e
f
g
h
K_0
W_0
Round 0
a
b
c
d
e
f
g
h
K_t
Wt
Round t
W79
a
b
c
d
e
f
g
h
K79
Round 79
+
+
+
+
+
+
+
+


1024 bits
M_1
XOR
W_0
W1
W15
W16
W80



$$W_t = \sigma_1^{512}(W_{t-2}) + W_{t-7} + \sigma_0^{512}(W_{t-15}) + W_{t-16}$$

Where,

$\sigma_0^{512}(x) = ROTR^1(x) \oplus ROTR^8(x) \oplus SHR^7(x)$

$\sigma_1^{512} = ROTR^{19}(x) \oplus ROTR^{61}(x) \oplus ROTR^6(x)$

$ROTR^N(x)$ = circular right shift (rotation) of the 64-bit argument x by n bits.

$SHR^N(x)$ = left shift of 64-bits arguments x by n bits with padding by zeros on write.

+= addition modulo 2^{64}

T_1 = h ch(e.f.g) +$(\sum_{1}^{512} e)$ + $W_t + K_t$

T_2 = $(\sum_{1}^{512} a)$ + Maj(a,b,c)

h=g

g=f

f=e

e= d+T_1

d= c

c=b

b=a

a= $T_1 + T_2$

Majority function

$(A_j \text{ AND } B_j) \oplus (B_j \text{ AND } C_j) \oplus (C_j \text{ AND } A_j)$

CONDITIONAL FUNCTION

$(E_j \text{ AND } F_j) \oplus (\text{not } E_j \text{ AND } G_j)$

ROTATE(E): $ROTR_{28}(E) \oplus ROTR_{34}(E) \oplus ROTR_{29}(E)$

ROTATE(A): $R_0 + R_{28}\ (A) \oplus ROTR_{34}(A) \oplus ROTR_{29}(A)$